



# CYBERSECURITY IM BETRIEB VON STROMNETZEN

*Dr. Stephan Hutterer*

*Produktmanager*



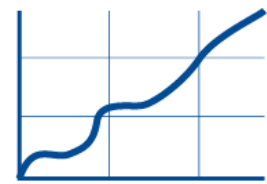
Unternehmen in Privatbesitz



5 Eigentümer (Management)



11 Standorte, HQ in Linz / A



GJ 17/18: AE ~ 78 Mio€

UM ~ 73 Mio€



~ 500 Mitarbeiter

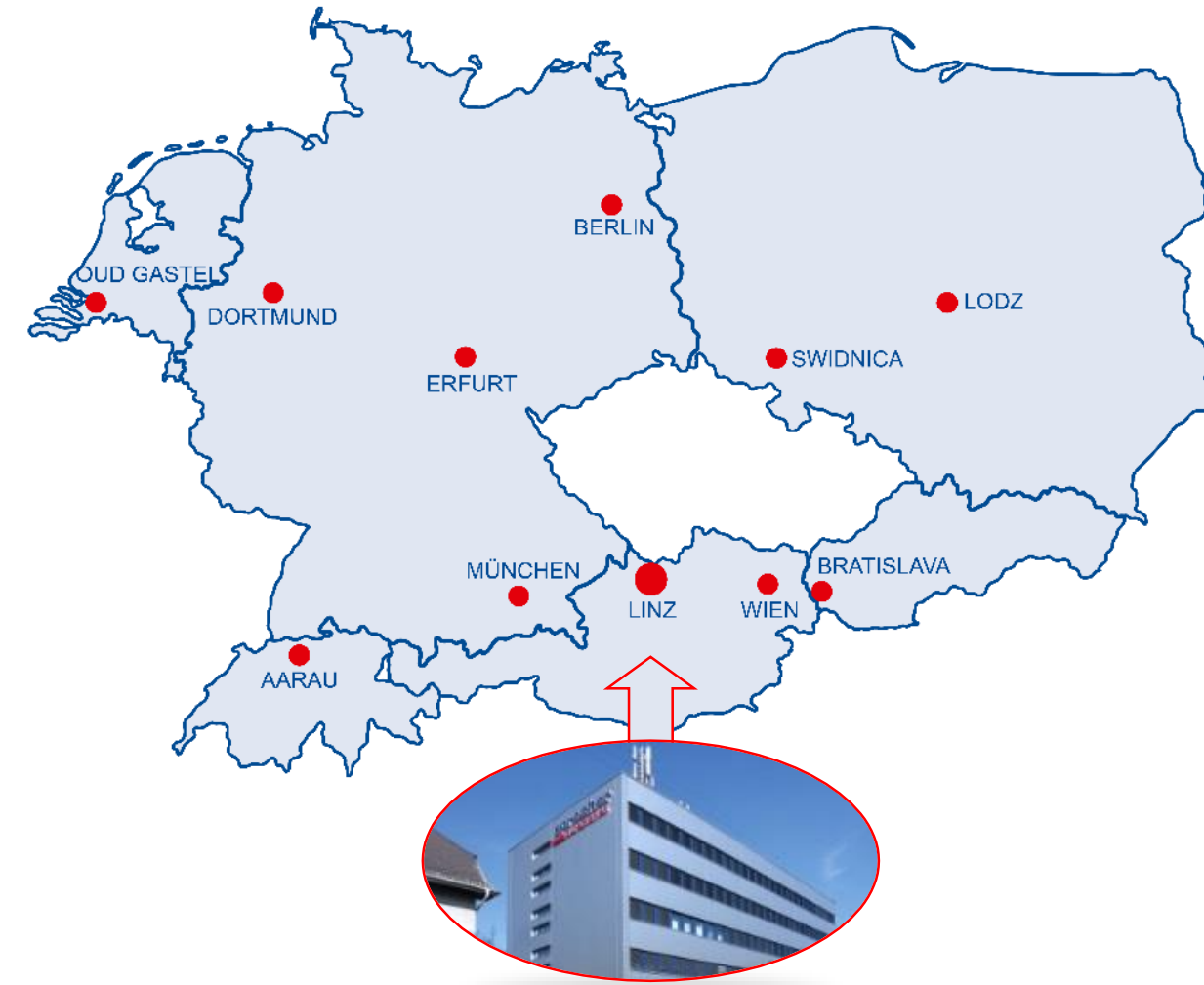


~ 40% der Mitarbeiter als stille Gesellschafter



## Wesentliche Leitlinien

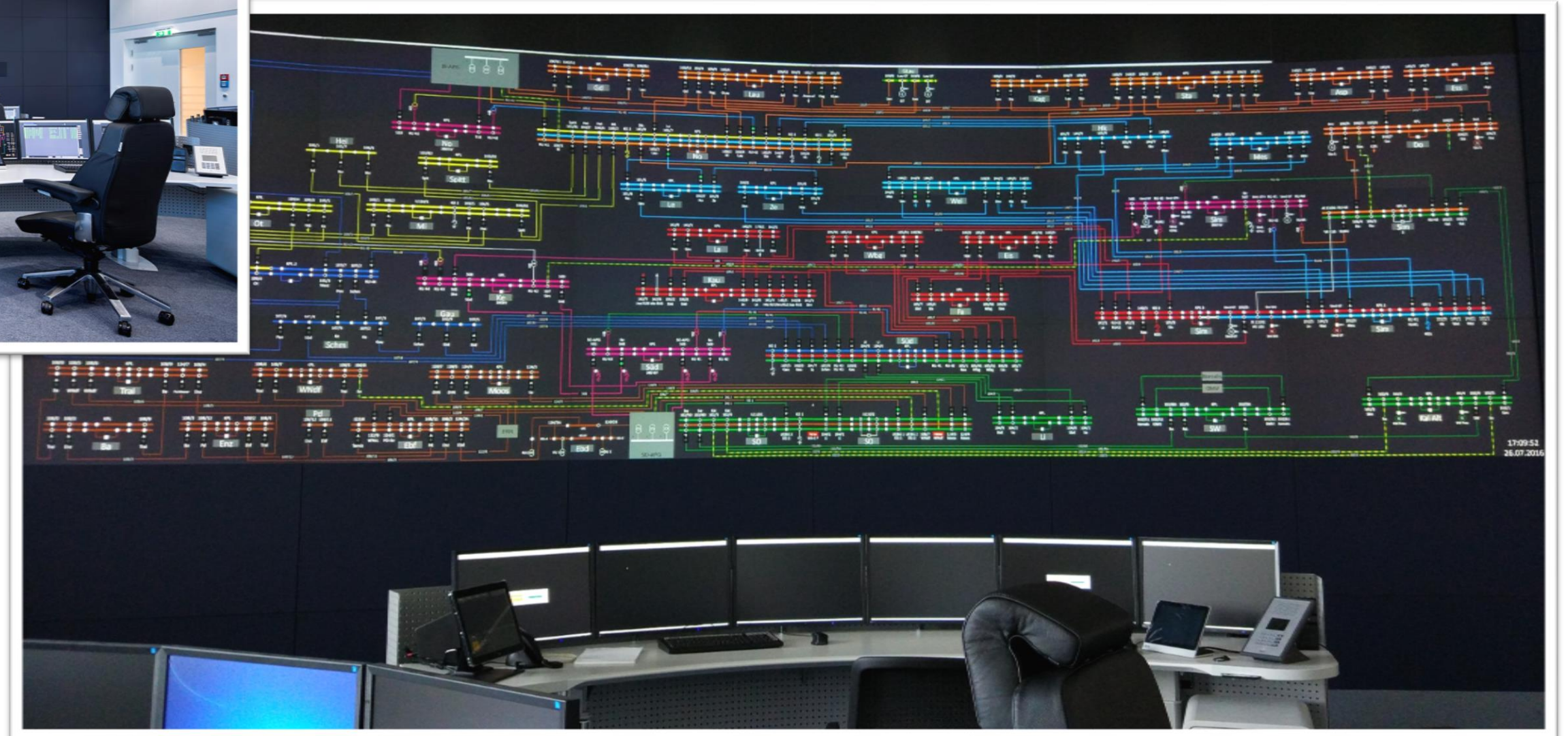
- Zukunftsorientierte Unternehmensentwicklung anstatt schneller Profite bzw. Profitmaximierung
- R&D in Österreich und Deutschland (~ 25% der Sprecher Ingenieure arbeiten ständig R&D)
- Produktion 100% in Österreich
- Lokalisierung der Produkte und Applikationssoftware durch unsere Standorte oder Partner



# SCHWERPUNKT "STROMVERSORGUNG"



# ENERGIEAUTOMATISIERUNG?



# ENERGIEAUTOMATISIERUNG?




# ENERGIEAUTOMATISIERUNG?




WAN

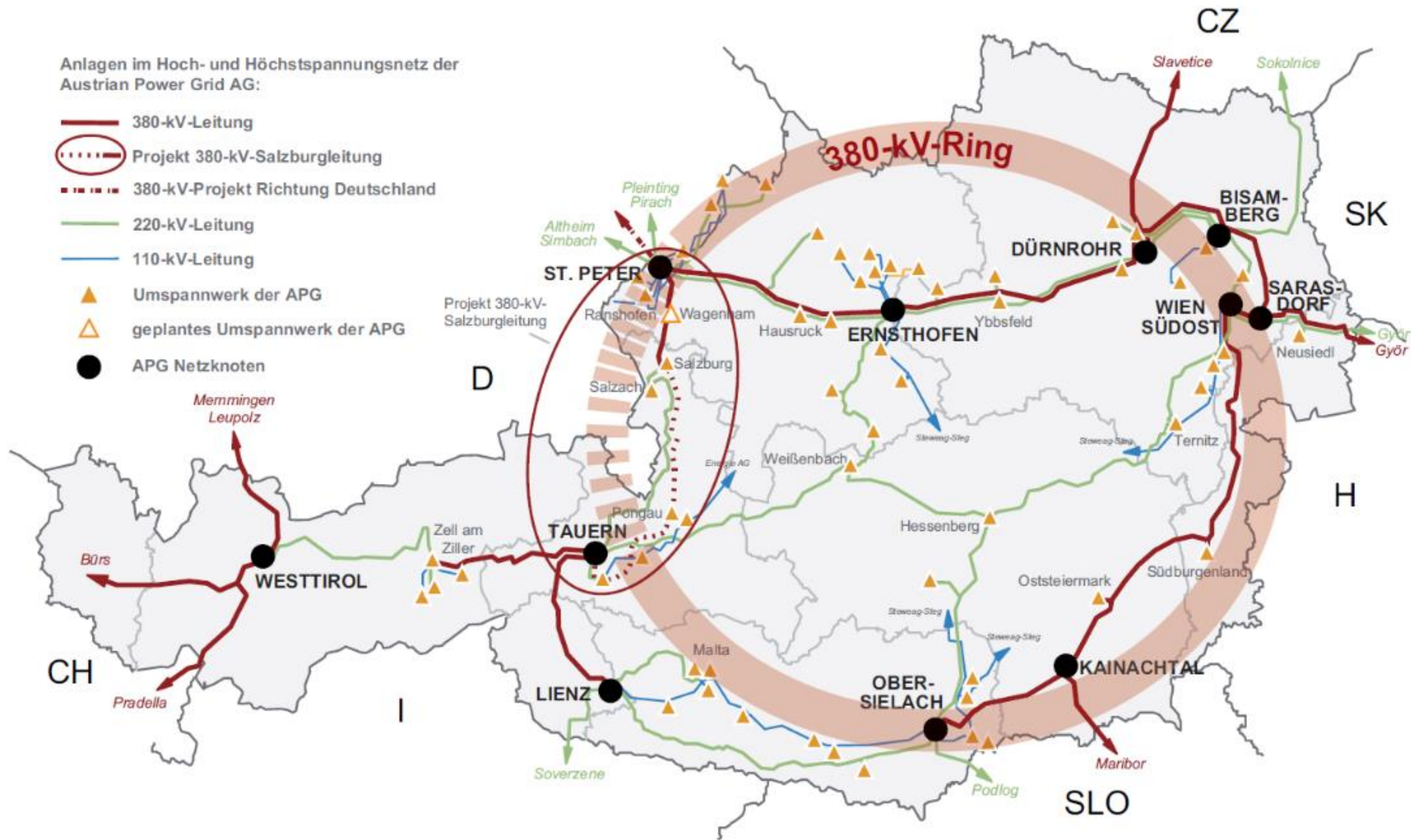
Dezentrale Einrichtung



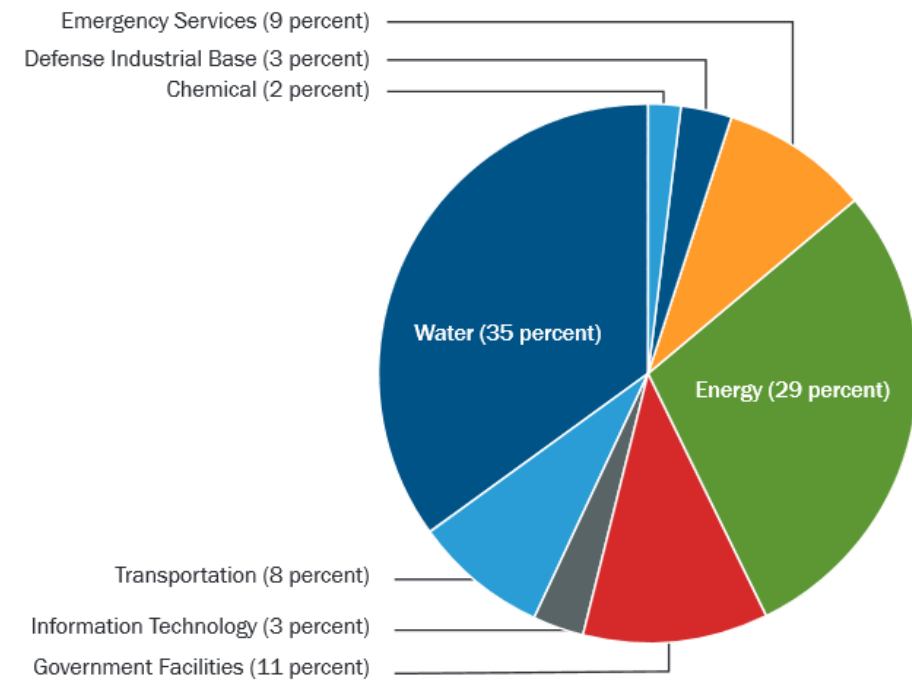
LAN / Hartverdrahtet



# STARK VERTEILTE NETZWERKE



# CYBERSECURITY: RELEVANT?



ICS CERT: FY2015 Industrial Control Systems Assessment Summary Report

Fokus auf kritische  
Infrastruktur nimmt zu



Network and Information Security (NIS) Directive

<https://secludit.com/blog/directive-network-and-information-security-sanctions/>



Gesetzliche Forderungen  
entstehen



Friday, February 5, 2016

## Experts compete to find Ukraine grid hack 'smoking gun'

*Following article has been re-published with the permission of Energy Wire  
(original text available at <http://www.eenews.net/energywire/stories/1060031555/>)*

### Experts compete to find Ukraine grid hack 'smoking gun'

Blake Sobczak, E&E reporter  
Published: Monday, February 1, 2016

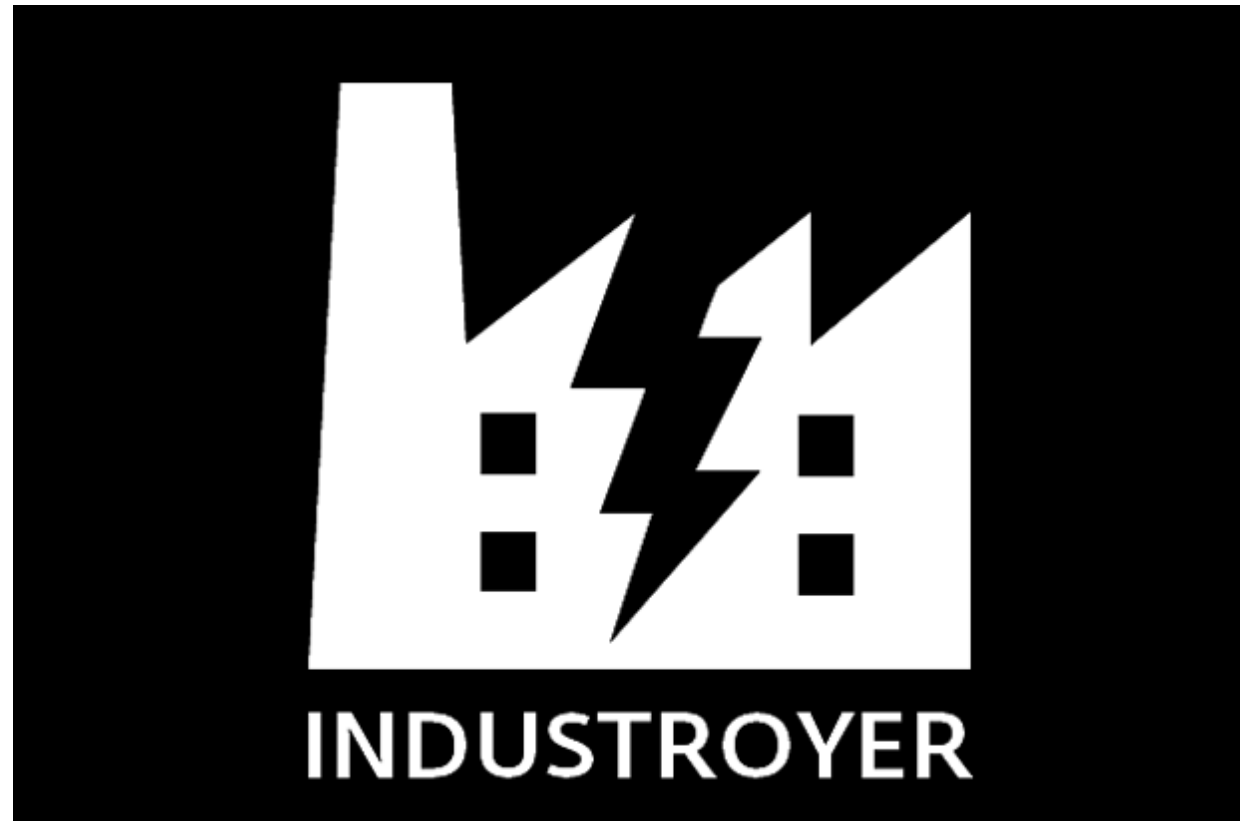
A six-hour blackout in western Ukraine has continued to puzzle investigators weeks after the lights came back on.

The Dec. 23 power outage in Ukraine's Ivano-Frankivsk region was minor by most standards, severing electricity to 80,000 households. Half a world away, windstorms were busy knocking out power to more than twice as many utility customers in northern Michigan.

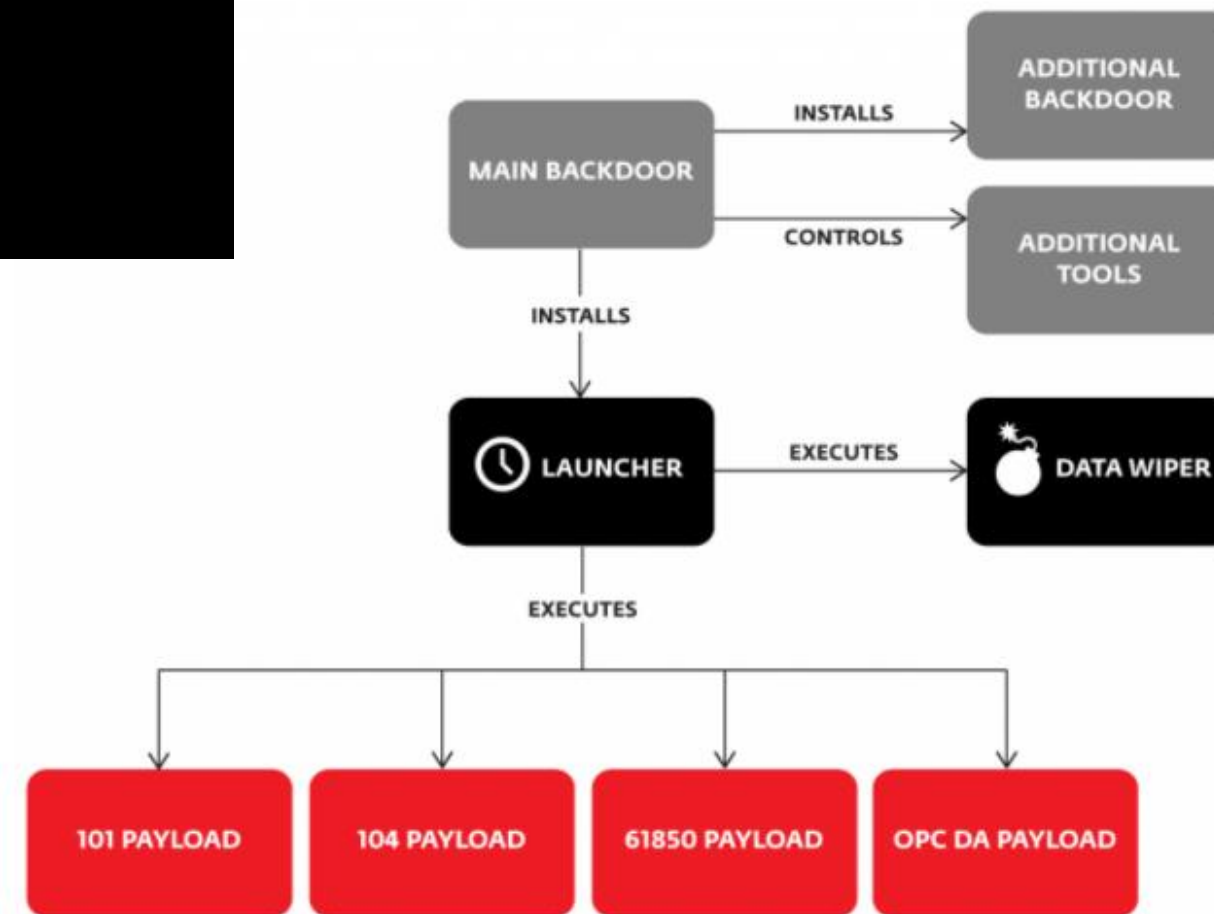
But Ukraine's outage that day resulted from a complex attack combining malware, a flood of telephone calls and, perhaps, a few unwitting accomplices in grid control centers.

Ukrainian officials are dissecting the BlackEnergy strain of malware found to have infected energy, media and government organizations across the country. Authorities haven't yet offered a detailed account of Dec. 23's events, so security researchers have pieced together their own – sometimes competing – versions of what happened.

# DOMÄNENWISSEN WIRD DEZIDIERT AUFGEBAUT

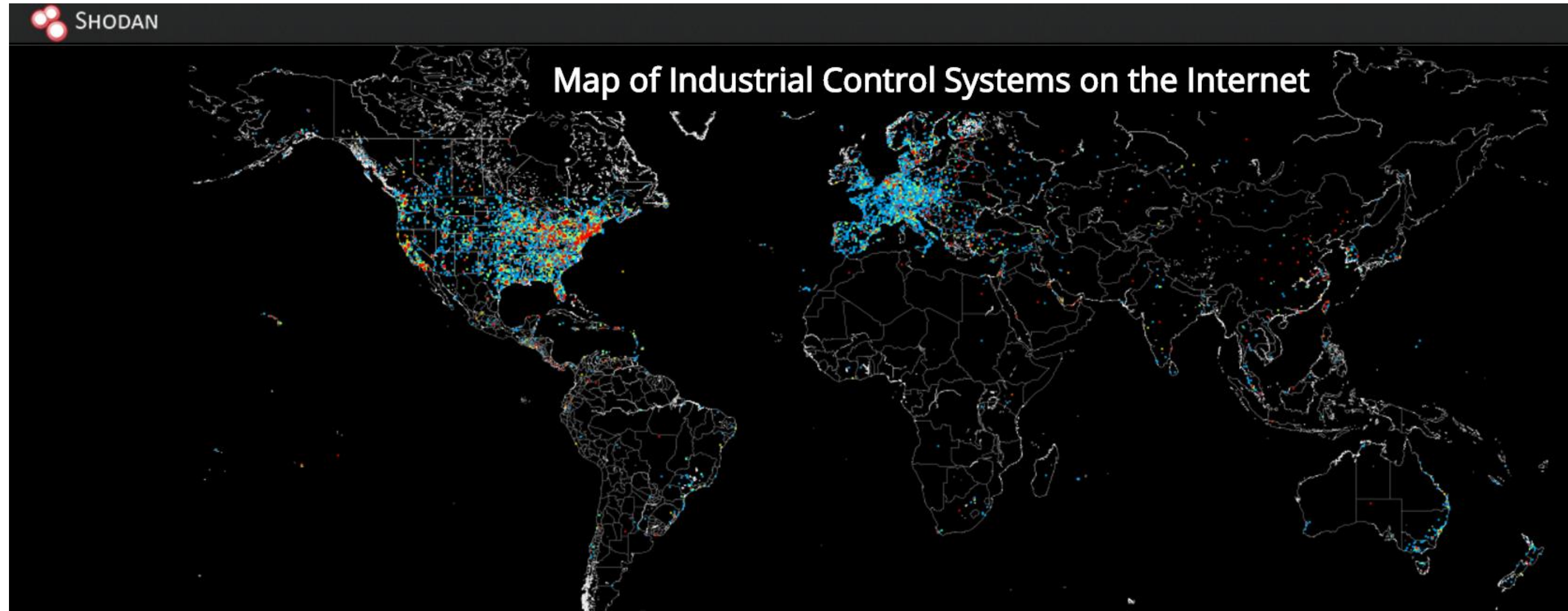


Source: [www.welivesecurity.com/](http://www.welivesecurity.com/)



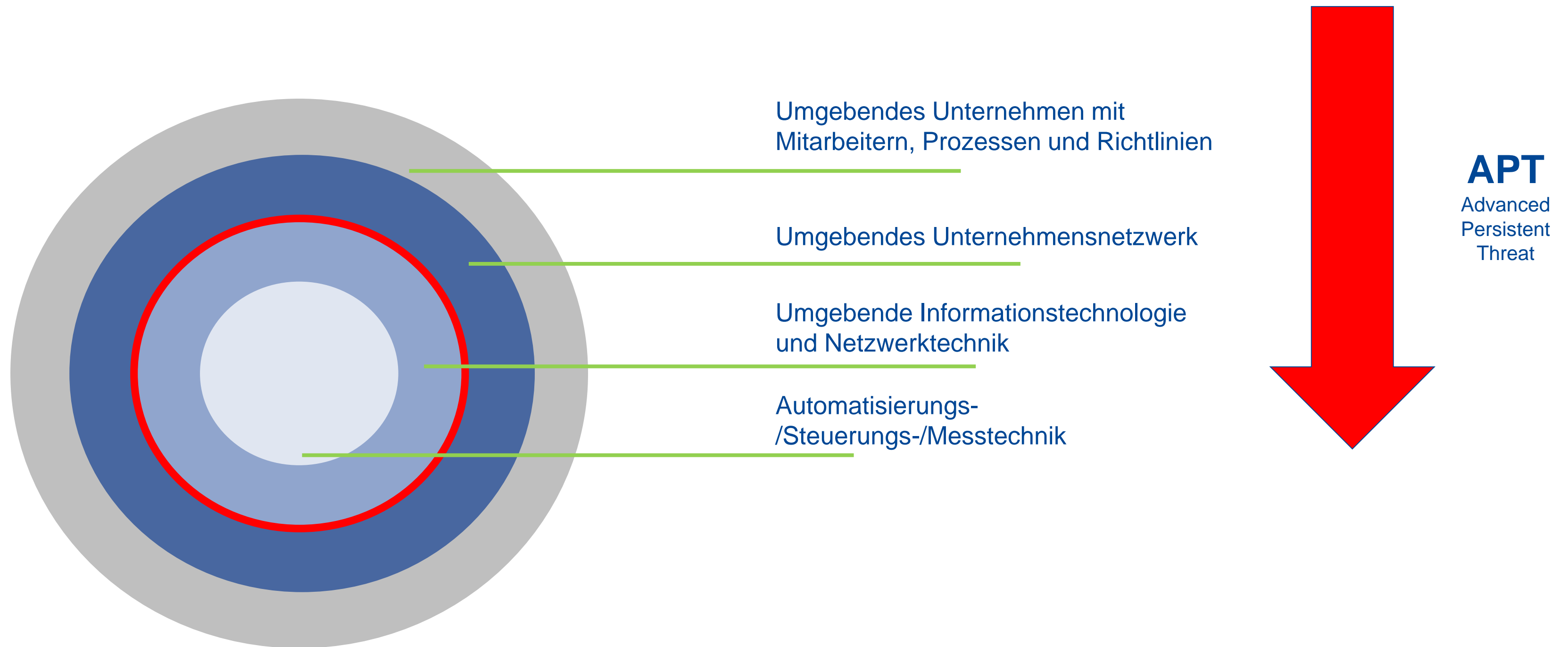
Source: ESET

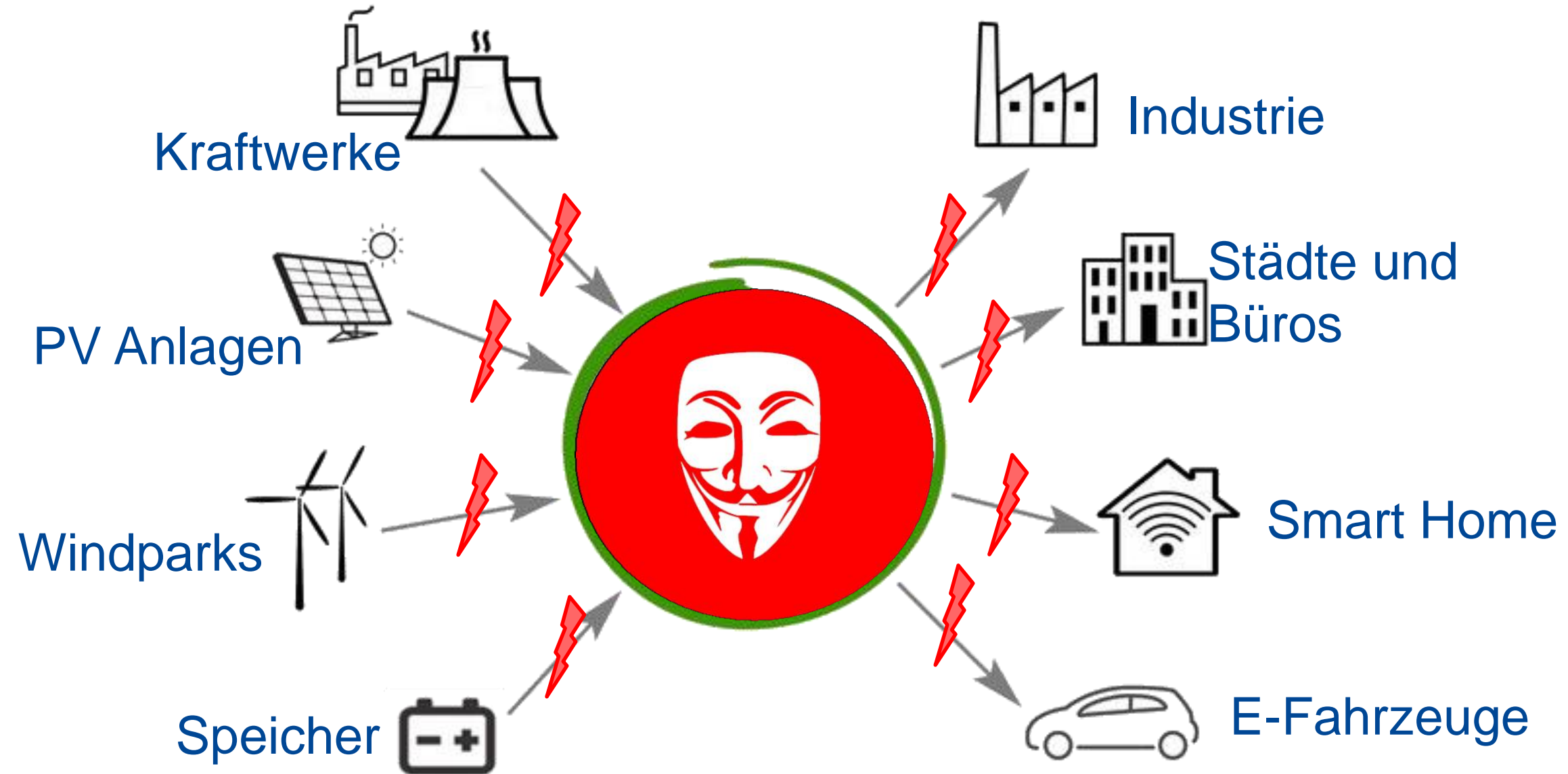
# BEWUSSTSEINSBILDUNG NOTWENDIG



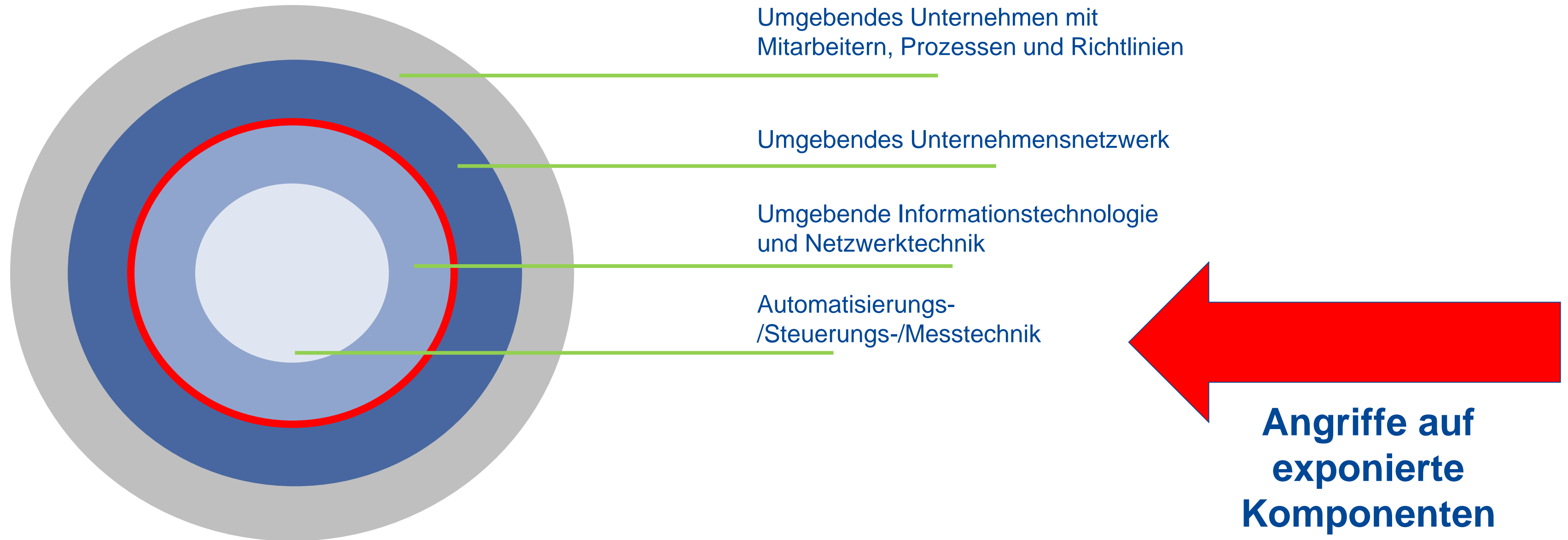
Source: <https://www.shodan.io/>

# SIND ANGRIFFE SCHWIERIG?



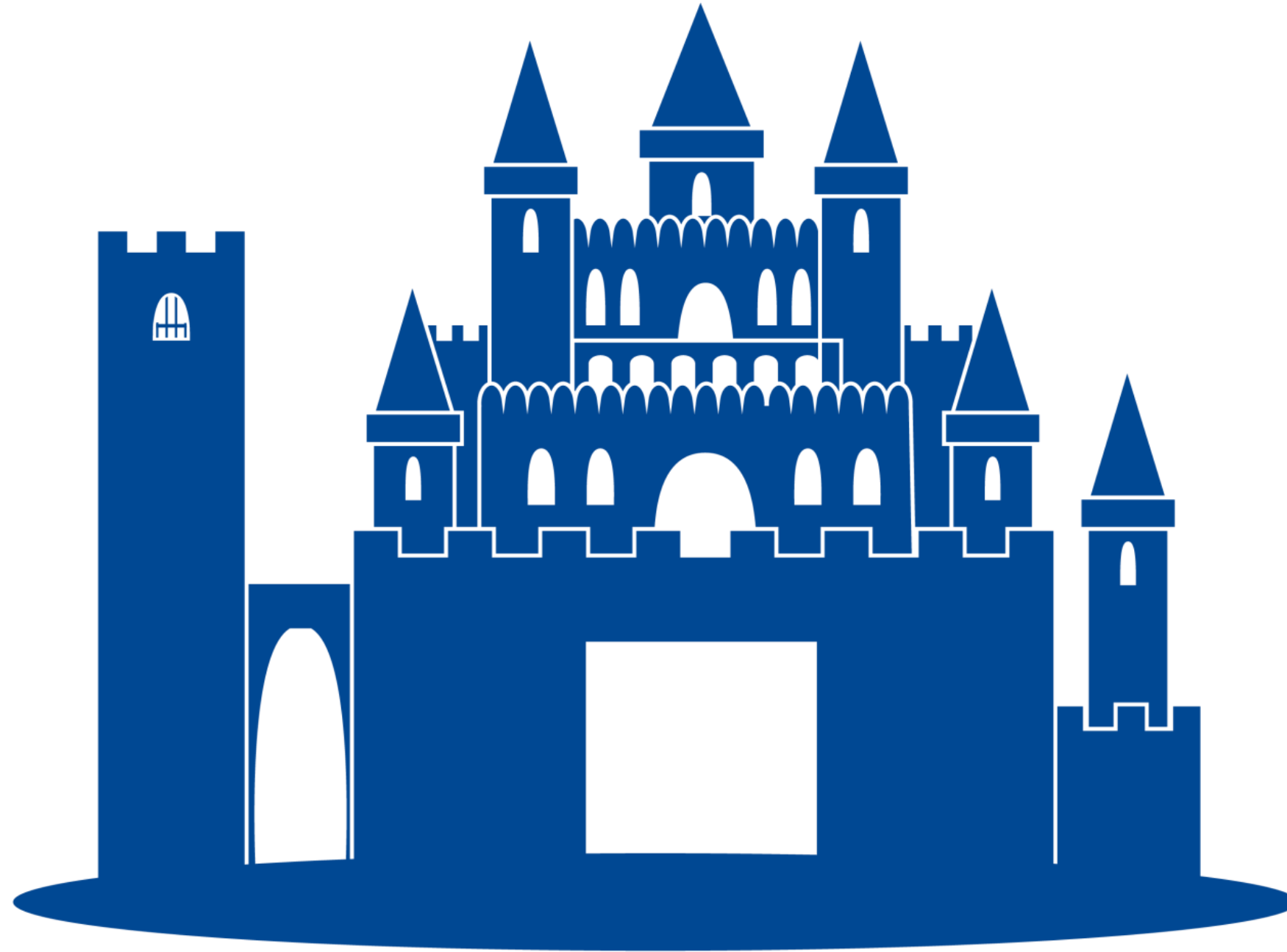


# WO LIEGT DAS RISIKO DURCH DIGITALISIERUNG?



# EIN SICHERHEITSKONZEPT WIRD BENÖTIGT

„DEFENSE IN DEPTH“



# VOLLSTÄNDIGE SYSTEMINTEGRATION



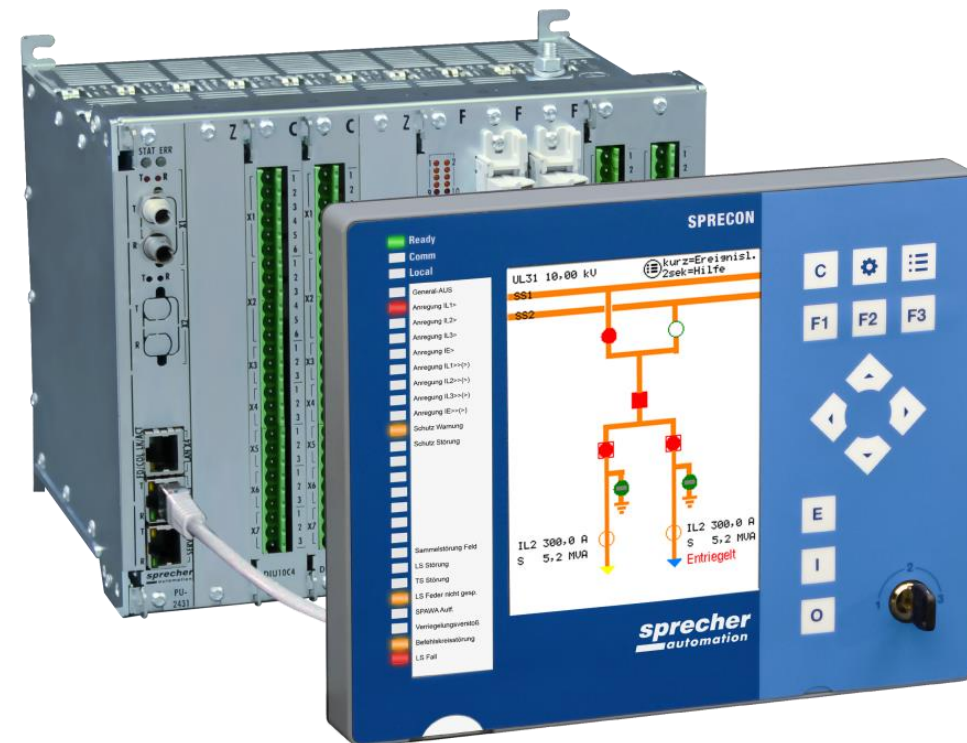
Systemhärtung



Verschlüsselung



Firewalls



Tunneling



Authentication &  
Authorization

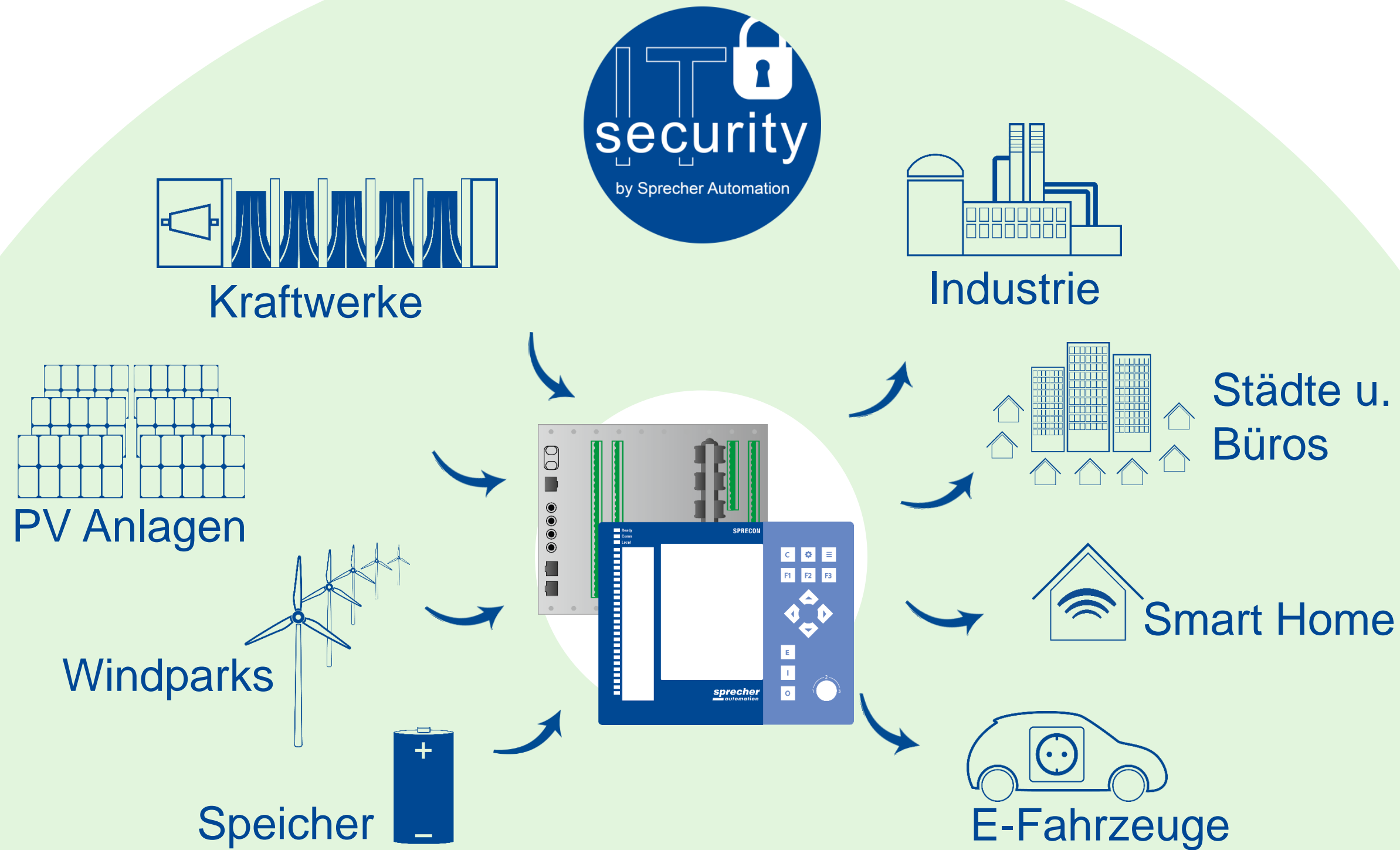


Patchmanagement



Security Monitoring /  
Intrusion Detection





**Für sichere Energieanlagen!**

**WE  
ARE  
HIRING**



# THANK YOU FOR YOUR ATTENTION

Any liability regarding the correctness and completeness of any information and/or specifications in the presentation is excluded. All rights are reserved to alter specifications, make modifications, or terminate models without prior notice. The specifications of a model may vary from country to country.